



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

hp

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/964,029	09/26/2001	Marcey L. Kelley	IL-10707	9891
7590	12/08/2005		EXAMINER	LEROUX, ETIENNE PIERRE
Eddie E. Scott Assistant Laboratory Counsel Lawrence Livermore National Laboratory P.O. Box 808, L-703 Livermore, CA 94551			ART UNIT	PAPER NUMBER
2161				
DATE MAILED: 12/08/2005				

Please find below and/or attached an Office communication concerning this application or proceeding.



UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
---------------------------------	-------------	---	---------------------

09/964,029	9/26/2001	Marcey L Kelley	1L-10707
EXAMINER			
Etienne LeRoux			
ART UNIT	PAPER		

2161 12052005

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

Attached is Examiner's Answer which is in response to Appeal Brief filed September 21, 2005

12052005



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

MAILED

Application Number: 09/964,029
Filing Date: September 26, 2001
Appellant(s): KELLEY ET AL.

DEC 08 2005

Technology Center 2100

Eddie E Scott
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed September 21, 2005 appealing from the Office action mailed May 5, 2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Bartoletti T., Dobbs LA, Melley M., "Secure Software Distribution System"
National Information Systems Security Conference Baltimore, MD October 6-7, 1997.
Paper printed February 1997 by Lawrence Livermore National Laboratory

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claim 6 is rejected under 35 U.S.C. 102(b) as being anticipated by Conference

Publication: Secure Software Distribution System by T. Bartoletti et al (hereafter Bartoletti), as provided by appellant.

Claim 6:

Bartoletti discloses:

- determining which of said software patches should be applied to said client's systems
[page 4, par 2, line 2]
- collecting said software patches from said vendors by downloading them from said vendor's ftp sites [page 5, par 1]
- determining which of vendor's upgrades and patches have been applied to client's systems [page 4, par 2, line 2]
- determining which said software upgrades and patches should be or should have been applied to said clients systems [page 4, par 2, line 2]

Art Unit: 2161

- collection of said patches and upgrades from said vendor's and downloading said patches and upgrades to client systems [page 4, par 1, lines 4,5]
- determining how much memory is needed to install said patch and upgrades [page 4, par 2, line 5]
- determining how dependencies on other layered products affect the installation of said patches and upgrades [page 4, par 2, line 6]
- determining how dependencies on other patches, or software upgrades affect the installation of a patch [page 4, par 2, line 6]
- determining how dependencies on other software upgrades affect the installation of a patch [page 4, par 2, lines 4-6]
- determining which files will be affected by the installation of a patch [page 4, par 2, lines 4-6],
- determining which directories will be affected by the installation of a patch [page 4, par 2, line 7]
- backing-out said software patches that have been applied to said client's systems [page 4, par 1, line 3, par 3]
- checking the permissions and ownership of the files referenced in the patch and ensuring that the system is authentic [page 5, par 1, line 12]
- determining which software patches should be installed by determining the needed software patches and the not needed software patches [page 6, par 2, line 16]
- distributing said needed software patches to said client's systems [page 6, par 2 line 18-20],

- installing said needed software patches [page 6, par 2, lines 18-20]

Response to Arguments

Appellant's arguments in Appeal Brief filed September 21, 2005 have been fully considered but they are not persuasive for the following reasons:

Appellant Argues:

Appellant states in first paragraph of page 10 "Appellants claim element #20 requires two positive separate actions, *checking the permissions and the ownership of the files referenced in the vendor's software patch and ensuring that the system software is authentic.* The portion of the Bartoletti et al reference as quoted in the Final Office Action does not disclose these two positive separate actions. In particular, the Bartoletti et al reference does not disclose the claim limitation *ensuring that the system software is authentic.*"

Examiner Responds:

Examiner is not persuaded. MPEP § 2106 requires Office personnel to give claims their broadest reasonable interpretation in light of the supporting disclosure. *In re Morris*, 127 F.3d 1048, 1054-55, 44 USPQ2d 1023, 1027-28 (Fed Cir. 1997). The following is taken from the supporting disclosure:

[0026] Certain embodiments of the system are known as SafePatch secure distribution software system. This system provides automated analysis, distribution, and notification and installation of security patches on network-based computer systems. SafePatch determines what patches need to be installed. For the patches that are installed, SafePatch checks the permissions and ownership of the files referenced in the patch and ensures that the system software is authentic. SafePatch detects patch deficiencies and distributes needed patches as well as the appropriate installation script to client's systems, and optionally installs those patches.

Above excerpt from Appellant's disclosure shows checking permissions and ownership of the files ensures the system software is authentic. Turning now to the Bartoletti et al reference as referenced above, i.e., page 5, paragraph 1 which includes:

The SSDS administrator can specify which vendor sites to monitor and which patches to collect (e.g. security, recommended, all). For instance only Solaris 2.5+ security patches can be collected. These patches are then converted to a non-vendor specific, machine readable format and stored in a database. The process of converting patches will involve some human interaction until the vendors adopt a standard patch format. Patches stored in this format are referred to as patch specifications. A patch specification contains information such as the operating system type, version, and architecture as well as the permissions and ownership for each file and directory manipulated by the patch. A cryptographic checksum for each file is also included in the patch specification to be used for file identification during the evaluation process described later.

The above disclosure by Bartoletti et al teaches: (1) the SSDS administrator specifies approved vendor sites with respect to security, (2) a patch specification includes permissions, (3) a patch specification includes ownership of each file, (4) a cryptographic checksum for each file for file identification during the evaluation process. Based on the above disclosure by Bartoletti et al, examiner maintains that Bartoletti reads on the claim limitation *ensuring that the system software is authentic*. It is noteworthy that Appellant's specification in paragraph 26 (reproduced above) includes checking permissions and ownership of the files to ensure that the system software is authentic which is exactly the same process disclosed in the Bartoletti et al reference (page 5, paragraph 1, reproduced above) for ensuring that the system software is authentic.

Furthermore, examiner notes the following excerpts from the Bartoletti et al reference can be mapped to claim limitation ... *ensuring that the system software is authentic*.

The Abstract includes:

Art Unit: 2161

SSDS will assist with the **authentication** of software by comparing the system's objects with the patch's objectives.

The Paragraph joining pages 1 and 2 includes:

This system will allow a network administrator (and users) to query and upgrade the **software integrity** of hundreds of individual systems from a central point through largely automated means. The centralized software system will provide the following services for target systems:

Rapid system software “trust” determination

Paragraph No. 3 of page 2 includes:

The process SSDS will use to **authenticate** the software on a system is more reliable and secure than other vendor-specific tools. SSDS will compare the target system's objects with the objects from the patch to determine what is actually installed and what needs to be installed. This process ensures **accurate reporting of a system's patch status**. It also allows SSDS to identify objects that do not belong to either the original system distribution or to any released patches.

Paragraph No. 3 of page 3 includes:

Software management tools are very much needed to support the assessment and authentication of system software on a network as well as installing and upgrading system software. Wouldn't it be nice to know exactly which of you 250 systems are patched up-to-date, which are not, and what patches are needed for each system. Sadly, there are many organizations where an administrator of 250 systems could not determine this in months time, and certainly not in a manner that involved actual examination of installed binary files. SSDS will enable an administrator to produce this information within hours of the request, from a single console designed to support this type of inquiry and it will do so by actually **examining the files present on these systems**.

Paragraph No 5, page 3 includes:

A software management tool should also support software re-authentication on a regular basis, commensurate in frequency with the value of resources being maintained on the systems. The SSDS project will provide system administrators with a fast and highly automated method to

authenticate system software, determine security patch versions and detect instances of subsequent tampering.

Paragraph 1, page 5 includes:

A patch specification contains information such as the operating system type, version and architecture as well as the **permissions and ownership** for each file and directory manipulated by the patch. A cryptographic checksum for each file is also included in the patch specification to be used for **file identification** during the evaluation process described later.

Appellant Argues:

Appellant maintains in the fifth paragraph of page 10 that claim element #21 requires two positive separate actions per the claim limitations *determining which of the vendor's software patches should be installed by determining the needed vendor's software patches*" and ... *the not needed vendor's software patches*. Particularly, appellant maintains the Bartoletti et al reference cited by the examiner in the Final Office Action does not disclose the following claim element *the not needed vendor's software patches*.

Examiner Responds:

Examiner is not persuaded. It is inherent that when the software patches that are needed are determined the patches that are not needed are also determined. However, in the following disclosure by Bartoletti, i.e., second paragraph of page 6, the Bartoletti et al teaching can be mapped to the claim limitation *the not needed vendor's software patches*.

This check permits the SSDS Server to determine which patches are actually installed on the target system without relying on the system's local database. From this information, the SSDS Server can determine which patches need to be installed on the target system in order to bring it up-to-date. The system administrator can choose to have SSDS install patches immediately after the evaluation or at some time later. The **system administrator can also chose not to have the SSDS install the patches** and instead report on the patches needed. This allows for the system administrators to dictate which actions SSDS is to perform on a system.

Bartoletti et al discloses per the bolded section in the above that the system administrator can choose not to have the SSDS install the patches which reads on the claim limitation
and the not needed vendor's software patches.

Furthermore, the following excerpts from the Bartoletti et al reference are relevant to the claim limitation *and the not needed vendor's software patches.*

Paragraph 1, page 4 includes:

A software management tool must be capable of collecting upgrades and patches; determining which upgrades and patches should be or have been applied to a system: and installing and possibly **backing-out upgrades and patches**.

Paragraph 2, page 6 includes:

The SSDS server controls the execution of a request by gathering information from the target systems and giving instructions to install and **back-out a patch**.

Paragraph 5, page 9 includes:

Finally, the third phase of the project will focus on the automated installation and backing-out of patches. [.....] Future extensions may support license-tracking to **detect the presence of unlicensed software applications**.

Appellant Argues:

Appellant maintains in the first paragraph of page 11 that the Bartoletti et al reference does not disclose the claim limitation *distributing the needed vendor's software patches to the client's systems*. Appellant subsequently quotes the following disclosure by Bartoletti et al, i.e., the disclosure relied upon in the Final Rejection Office Action mailed May 5, 2005 and suggests that the disclosure cannot be mapped to the claim limitation.

The system administrator can choose to have SSDS install patches immediately after the evaluation or at some later date and time. The system administrator can also choose not to have

SSDS install the patches and instead report on the patches needed. This allows for the system administrators to dictate which actions SSDS is to perform on a system." (Page 6, paragraph 2, lines 18-20, Secure Software Distribution System by Tony Bartoletti, Lauri A. Dobbs, and Marcey Kelley, National Information Systems Security Conference Baltimore, MD, October 6-7, 1997)

Examiner Responds:

Examiner is confused. Examiner maintains above disclosure which teaches that the system administrator "can choose to have SSDS install patches immediately" can be accurately mapped to the claim limitation*distributing the needed vendor's software patches to the client's systems.* Furthermore, the following excerpts from the Bartoletti et al reference are pertinent to the claim limitation *distributing the needed vendor's software patches to the client's systems.*

The Abstract includes:

SSDS will assist with the authentication of software by comparing the system's objects with the patch's objects. SSDS will monitor vendor's patch sites to determine when the new patches are released and **will upgrade system software on target systems automatically.**

Paragraph 3, page 4 includes:

If the patch is applicable to the system, **then the software management tool can install the patch or upgrade.**

Paragraph 2, page 7 includes:

Here one or two computers would be configured to **support the patch collection and storage function of the SSDS Server.**

Paragraph 3, page 7 includes:

Art Unit: 2161

These systems would get their patches from the centralized patch collectors (see Figure 2). The SSDS Client software would be installed on all systems in the network. This configuration distributes the work load and reduces duplication of effort.

Appellant Argues:

Appellant maintains in the second paragraph of page 12 that the Bartoletti reference is not an "enabled reference" because the invention defined by the method steps of the claims on appeal are not supported in the Bartoletti et al by a description of how the method is implemented.

Examiner Responds:

Examiner is not persuaded. Examiner maintains the disclosure in the Bartoletti et al reference is enabling because one of ordinary skill in the art would be able to make the present invention based on the Bartoletti et al reference. In fact, this is exactly what happened when skilled technicians i.e., Tony Bartoletti, Lauri A. Dobbs and Marcey Kelley, consulted conference paper titled "Secure Software Distribution System" which was presented at the National Information Security Systems Security Conference in Baltimore, MD on October 6-7, 1997 and were thus enabled to further develop the subject matter in order to make the present invention. Appellant provides no argument why Tony Bartoletti, Lauri A. Dobbs and Marcey Kelley cannot be characterized as skilled technicians and thus examiner concludes that the Bartoletti et al reference is enabling such that one of ordinary skill in the art would be able to make the present invention.

For the above reasons, it is believed that the rejections should be sustained.

Art Unit: 2161

Respectfully submitted,

Conferees:

Safet Metjahić

Supervisory Patent Examiner
AU 2164

C. Rones

Charles Rones

Supervisory Patent Examiner
AU 2164

Etienne LeRoux

AU 2161

E.J. Lehman

J. M.

An appeal conference was held on December 1, 2005 with above conferees in attendance